DATE(S) ISSUED:

8/25/2010

SUBJECT:

Multiple Vulnerabilities in Adobe Shockwave Player Could Allow Remote Code Execution

OVERVIEW:

Adobe has provided an update which addresses multiple vulnerabilities in Adobe Shockwave Player. These vulnerabilities could allow an attacker to take complete control of an affected system. Adobe Shockwave Player is a prevalent multimedia application used to display animations and video. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page. Exploitation may also occur when a user opens a specially crafted Shockwave (SWF) file. Successful exploitation will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Adobe Shockwave Player 11.5.7.609 and earlier

RISK:

Government:
  Large and medium government entities: **High**
  Small government entities: **High**

Businesses:
  Large and medium business entities: **High**
  Small business entities: **High**

Home users: High

DESCRIPTION:

Adobe has provided an update which addresses twenty security vulnerabilities in Adobe Shockwave Player. These vulnerabilities may be exploited if a user visits or is redirected to a specially crafted web page. Exploitation may also occur when a user opens a specially crafted Shockwave (SWF) file.

- There are 16 memory corruption vulnerabilities that could result in remote code execution.

- There are 2 denial-of-service vulnerabilities.

- A pointer-offset error vulnerability may result in remote code execution.

- An unspecified integer-overflow vulnerability could result in remote arbitrary code execution.

Successful exploitation of the remote code execution vulnerabilities will result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Systems running Adobe Shockwave Player 11.5.7.609 and earlier versions should be updated to version 11.5.8.612 immediately after appropriate testing.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Do not open email attachments from unknown or un-trusted sources.

REFERENCES:

Adobe:

http://www.adobe.com/support/security/bulletins/apsb10-20.html

http://get.adobe.com/shockwave/

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2863

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2864

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2865

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2866

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2867

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2868

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2869

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2870

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2871

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2872

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2873

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2874

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2875

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2876

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2877

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2878

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2879

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2880

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2881

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2882